Office of the Governor
State Chief Information Officer

SECURITY

Chapter 14 – Planning for Business Continuity

Scope: These standards apply to all public agencies, their agents or designees subject to Article 3D of Chapter 147, "State Information Technology Services."

Statutory Authority: N.C.G.S. 147-33.89

Section 01 Business Continuity Management

140101 Initiating the Business Continuity Plan (BCP)

Purpose: To establish the appropriate level of business continuity management to sustain the operation of critical business services following a disaster or adverse event.

STANDARD

Agencies, through their management, must implement and support an appropriate information technology business continuity program to ensure the timely delivery of critical automated business services to the State's citizens.

A management team composed of representatives from all the agency organizational areas has primary leadership responsibility to identify information technology risks and to determine what impact these risks have on business operations. Management must also plan for business continuity, including disaster recovery, based on these risks and document continuity and recovery strategies and procedures in a defined business continuity plan that is reviewed, approved, tested and updated on an annual basis.

ISO 17799: 2005 REFERENCE
14.1.04 Business continuity planning framework

140102 Assessing the BCP Risk

Purpose: To require that State agencies manage information technology risks appropriately.

STANDARD

Agencies shall identify the potential risks that may adversely impact their business in order to develop continuity and recovery strategies and justify the financial and human resources required to provide the appropriate level of continuity initiatives and programs.

Agencies shall conduct risk impact analysis activities that:

- Define the agency's critical functions and services.
- Define the resources (technology, staff and facilities) that support each critical function or service.
- Identify key relationships and interdependencies among the agency's critical resources, functions and services.
- Estimate the decline in effectiveness over time of each critical function or service.
- Estimate the maximum elapsed time that a critical function or service can be inoperable without a catastrophic impact.
- Estimate the maximum amount of information or data that can be lost without a catastrophic impact to a critical function or service.
- Estimate financial losses over time resulting from the inoperability of each critical function or service.
- Estimate tangible (nonfinancial) impacts over time resulting from the inoperability of each critical function or service.
- Estimate intangible impacts over time resulting from the inoperability of each critical function or service.
- Document any critical events or services that are time-sensitive or predictable and require a higher-than-normal priority (for example, tax filing dates, reporting deadlines, etc.).
- Identify any critical nonelectronic media required to support the agency's critical functions or services.
- Identify any interim or workaround procedures that exist for the agency's critical functions or services.

ISO 17799: 2005 REFERENCES

14.1.02	Business continuity and risk assessment
14.1.04	Business continuity planning framework

140103 Developing the BCP

Purpose: To require that the appropriate level of information technology business continuity management is in place to sustain the operation of critical information technology services to support the continuity of vital business functions.

STANDARD

Management shall develop a business continuity plan (BCP) that covers all of the agency's essential and critical business activities and that includes references to procedures to be used for the recovery of systems that perform the agency's essential and critical business activities.

At a minimum, an agency's business continuity plan shall**:**

- Help protect the health and safety of the employees of the State of North Carolina.
- Protect the assets of the State and minimize financial, legal and/or regulatory exposure.
- Minimize the impact and reduce the likelihood of business disruptions.
  - Crisis teams and response plans for threats and incidents.
  - Communication tools and processes.
- Require that employees are aware of their roles and responsibilities in the BCP and in plan execution.
  - Training and awareness programs.
  - Simulations and tabletop exercises.
- Have a documented policy statement outlining:
  - Framework and requirements for developing, documenting, and maintaining the plans.
  - Requirements for testing and exercising.
  - Review, sign-off and update cycles.
- Have senior management oversight and sign-off.
- Assess the professional capability of third parties and ensure that they provide adequate contact with the agencies.
- Review dependence on third parties and take actions to mitigate risk associated with dealing with third parties.
- Provide direction on synchronization between any manual work data and the automated systems that occur during a recovery period.
- Set forth procedures to be followed for restoring critical systems to production.

ISO 17799: 2005 REFERENCES

14.1.03	Developing and implementing continuity plans including information security
14.1.04	Business continuity planning framework

140104 Testing the BCP

Purpose: To ensure that management and staff understand how the business continuity plan is executed.

STANDARD

The agency business continuity plan shall be tested at least annually.

GUIDANCE

The following methods are recommended:

- Tabletop testing (walk-through of business recovery arrangements using example interruptions).
- Simulations (especially for postincident / postcrisis management roles).
- Technical recovery testing.
- Testing recovery at an alternate site.
- Testing of hot-site arrangements, complete rehearsal (testing organization, personnel, equipment, facilities and processes).
- Updating of plan as necessary.

Additional steps that may be taken include the rerunning of the test to validate any updated procedure(s) and the addition or removal of application backup procedures. The decision on what type of testing methodology to use should be defined, documented and approved by agency management. The agency is responsible for maintaining its ability to recover in the event of an outage.

ISO 17799: 2005 REFERENCES
14.1.04 Business continuity planning framework
14.1.05 Testing, maintaining and re-assessing business continuity plans

140105 Training and Staff Awareness on BCP

Purpose: To help employees understand the components of the business continuity plan and their roles in disaster planning and response.

STANDARD

Training and awareness programs shall be undertaken to ensure that the entire agency is confident, competent and capable and understands the roles each individual within the agency must perform in a disaster/adverse situation.

ISO 17799: 2005 REFERENCES
14.1.04 Business continuity planning framework
14.1.05 Testing, maintaining and re-assessing business continuity plans

140106 Maintaining and Updating the BCP

Purpose: To maintain an up-to-date business continuity plan that reflects actual business requirements.

STANDARD

The person(s) designated as the agency business continuity plan (BCP) coordinator(s) has (have) the responsibility of overseeing the individual plans and files that constitute the BCP and ensuring that they are current, meet best practices and are consistent with the agency's overall plan. At the direction of the State Chief Information Officer, an agency's BCP shall be reviewed periodically by the Office of Information Technology Services and recommendations shall be made for improvement, if necessary.

ISO 17799: 2005 REFERENCE
14.1.05 Testing, maintaining and re-assessing business continuity plans

HISTORY

Approved by State CIO: September 16, 2005
Original Issue Date: September 16, 2005

Subsequent History:

Standard Number	Version	Date	Change/Description

Old Security Policy/Standard	New Standard Numbers
Information Technology Business Continuity Management Policy	All of Chapter 14